AMENDMENTS TO THE CLAIMS

Please amend Claims 1, 15, 17-18, 20, 22-24, 26-27, 29-31, and 35-36 as follows and cancel Claims 13-14 and 37 as follows, without prejudice or disclaimer to continued examination on the merits:

1. (Currently Amended): A method for mapping the topology of a wireless network, the method comprising the steps of:

(a) receiving scan data comprising information collected from frames transmitted on the wireless network, wherein the received scan data is received from a wireless sensor configured to monitor the wireless network and collect information from frames transmitted on the wireless network, wherein the scan data is associated with monitoring of one or more wireless access points, one or more wireless network nodes or combinations thereof;

(b) identifying a relationship (1) between at least one of the wireless access points and at least one of the wireless network nodes or (2) between any two wireless network nodes based on the received scan data, a characteristic of at least one of the wireless access points, a characteristic of at least one of the wireless network nodes or combinations thereof, wherein the relationship is identified responsive to an analysis of the scan data and responsive to a relationship between the wireless sensor and a server; [[and]]

(c) storing the identified relationship, access point characteristic, node characteristic or combinations thereof in a system data store as topology data;

(d) formatting the stored topology data based upon a desired output format; and

(e) repeating steps (a) through (d) a plurality of times, wherein the system data store stores topology data for each repetition, and wherein potential security and policy violations are detected through a comparison of topology data from one repetition to another repetition.

2. (Original): The method of claim 1, and further comprising the step of initiating one or more scans of wireless transmissions to generate the scan data.

3. (Original): The method of claim 2, wherein the step of initiating one or more scans comprises initiating a plurality of scans.

4. (Original): The method of claim 3, wherein each of the plurality of scans is initiated upon a different wireless sensor.

5. (Original): The method of claim 4, wherein each of the plurality of scans occurs simultaneously.

6. (Original): The method of claim 4, and further comprising the step of repeating the step of initiating the plurality scans.

7. (Original): The method of claim 6, wherein the repetition step occurs over a particular time period.

8. (Original): The method of claim 7, and further comprising the step of determining the particular time period based upon configuration data, network security threat level, current network activity, historical network activity or combinations thereon.

9. (Original): The method of claim 3, wherein each of the plurality of scans occurs within a particular time period.

10. (Original): The method of claim 9, and further comprising the step of determining the particular time period based upon configuration data, network security threat level, current network activity, historical network activity or combinations thereof.

11. (Original): The method of claim 2, and further comprising the step of receiving a mapping request from a user or a computer and wherein the scan initiation step is responsive to the received mapping request.

12. (Original): The method of claim 2, wherein the one or more initiated scans are initiated continuously or at periodic intervals.

13. (Canceled)

14. (Canceled)

15. (Currently Amended): The method of claim 1 [[13]], and further comprising the step of [[(e)]] (f) storing the formatted topology data in a data store accessible by a server system.

16. (Original): The method of claim 15, wherein the server system is an HTTP server, a WAIS server, a gopher server, or an FTP server.

17. (Currently Amended): The method of claim 1 [[13]], wherein the desired output format is TIFF, GIF, JPEG, HTML, SMS, MIME, S/MIME, ZIP, SML, SGML, WAP, BMP or combinations thereof.

18. (Currently Amended): The method of claim 1 [[13]], and further comprising the step of receiving a mapping request and wherein the formatting step is responsive to the received mapping request.

19. (Original): The method of claim 18, wherein the mapping request is received from a user or a computer system.

20. (Currently Amended): The method of claim 1 [[13]], and further comprising detecting a mapping trigger event based upon the received scan data and wherein the formatting step is responsive to the detected trigger event.

21. (Original): The method of claim 20, wherein the trigger event is a usage volume anomaly, a connectivity pattern anomaly, a policy violation, a security violation or combinations thereof.

22. (Currently Amended): The method of claim 1, and further comprising the step of [[(d)]] (f) transmitting the stored topology data to a desired output device.

23. (Currently Amended): The method of claim 22, and further comprising the step of repeating steps (a) through [[(d)]] (f) a plurality of times.

24. (Currently Amended): The method of claim 22, and further comprising the steps of [[(e)]] (g) determining a desired output format and [[(f)]] (h) formatting the stored topology data based upon the desired output format prior to transmission.

25. (Original): The method of claim 24, wherein the step of determining the desired output format comprises the step of determining the desired output format based upon configuration data, the desired output device, a mapping request or combinations thereof.

26. (Currently Amended): The method of claim 22, and further comprising the step of [[(e)]] (g) determining the desired output device.

27. (Currently Amended): The method of claim 26, wherein step [[(e)]] (g) comprises the step of determining the desired output device based upon configuration data, a mapping request or combinations thereof.

28. (Original): The method of claim 22, wherein the desired output device is a monitor, a printer, a further processing system, a pager, a telephone, a personal data assistant (PDA), an e-mail account or a combination thereof.

29. (Currently Amended): The method of claim 22, wherein the desired output device is capable of rendering graphical output and further comprising the step of [[(e)]] (g)

formatting the topology data in a manner to graphically represent characteristics or relationships prior to transmission;

wherein the graphically represented characteristics or relationships comprise whether a wireless access point of the one or more wireless access points is authorized, unauthorized, or ignored and whether a wireless network node of the one or more wireless network nodes is authorized, unauthorized, unassociated, an adhoc station, or ignored.

30. (Currently Amended): The method of claim 29, wherein the desired output device is capable of rendering color output and wherein the formatting step [[(e)]] (g) comprises the step of formatting the topology data in manner using color to represent characteristics or relationships prior to transmission.

31. (Currently Amended): The method of claim 22, wherein the desired output device is capable of rendering color output and further comprising the step of [[(e)]] (g) formatting the topology data in manner using color to represent characteristics or relationships prior to transmission.

32. (Original): The method of claim 1, and further comprising the step of identifying a relationship between a plurality of the wireless nodes based on the received scan data in which no wireless access point is involved.

33. (Previously Presented): A system for mapping the topology of a wireless network, the system comprising:

(a) storage means for storing topology data comprising access point characteristic data, wireless network node characteristic data, access point to node relationship data, node to node relationship data or combinations thereof;

(b) a wireless sensor for scanning wireless transmissions within a wireless network and generating scan data therefrom, wherein the scan data comprises information collected from frames transmitted on the wireless network;

(c) receiving means for receiving scan data from the wireless sensor over one of a wireless and wired connection;

(d) analysis means for generating topology data by identifying from scan data received by the receiving means a characteristic of a wireless network node, a characteristic of an access point, a characteristic of the wireless sensor, an access point to node relationship, a node to node relationship, an access point to sensor relationship, a node to sensor relationship, or combinations thereof and for storing the generated topology data in the storage means;

(e) output means for formatting topology data generated by the analysis means based upon a desired output format and for transmitting the formatted topology data to a desired output device; and

(f) topology comparison means for comparing topology data to prior topology data to evaluate potential security and policy violations of the wireless network.

34. (Previously Presented): The system of claim 33, further comprising intrusion detection means for detecting a usage volume anomaly, a connectivity pattern anomaly, a policy violation, a security violation or combinations thereof, and wherein the output means is responsive to a mapping request from a trigger event from the intrusion detection means.

35. (Currently Amended): The system of claim 33, further comprising intrusion detection means for detecting a usage volume anomaly, a connectivity pattern anomaly, a policy violation, a security violation or combinations thereof, and wherein the wireless sensor monitors ~~monitoring means is~~ responsive to a mapping request from a trigger event from the intrusion detection means.

36. (Currently Amended): A system for mapping the topology of a wireless network, the system comprising:

(a) a system data store (SDS) capable of storing topology data comprising access point characteristic data, wireless network node characteristic data, access point to node relationship data, node to node relationship data or combinations thereof; [[and]]

(b) a system processor comprising one or more processing elements, wherein the system processor is in communication with the SDS and wherein the one or more processing elements are programmed or adapted at least to:

(1) initiate at least one scan of one or more wireless access points, one or more wireless network nodes or combinations thereof, wherein the at least one scan is performed by a wireless sensor configured to monitor the wireless network and collect information from frames transmitted on the wireless network;

(2) receive scan data comprising information collected from frames transmitted on the wireless network, and wherein the scan data is associated with monitoring of one or more wireless access points, one or more wireless network nodes or combinations thereof;

(3) identify a relationship (i) between at least one of the wireless access points and at least one of the wireless network nodes or (ii) between any two wireless network nodes based on the received scan data, a characteristic of at least one of the wireless access points, a characteristic of at least one of the wireless network nodes or combinations thereof, wherein the relationship is identified responsive to an analysis of the scan data and responsive to a relationship between the wireless sensor and a server;

(4) store the identified relationship, access point characteristic, node characteristic or combinations thereof in the SDS as topology data; and

(5) format topology data generated based upon a desired output format; and

(6) output the formatted topology data to a desired output device;

(c) a wireless receiver that monitors wireless transmissions, wherein the wireless receiver is in communication with the system processor and wherein the system processor's programming or adaptation to initiate at least one scan includes at least programming or adaptation to initiate the scan using the wireless receiver and wherein its programming or adaptation to receive scan data includes at least programming or adaptation to receive scan data from the wireless receiver or from an interface therewith; and

(d) an intrusion detection engine configured to detect a usage volume anomaly, a connectivity pattern anomaly, a policy violation, a security violation or combinations thereof;

wherein an iteration of steps (1) through (6) is initiated responsive to the intrusion detection engine detecting a violation.

37. (Canceled)

38. (Previously Presented): One or more computer-readable media storing instructions that upon execution by a system processor cause the system processor to map the topology of a wireless network by performing at least the steps comprising of:

(a) initiating a scan of one or more wireless access points, one or more wireless network nodes or combinations thereof, wherein the scan is performed by a wireless sensor configured to monitor the wireless network and collect information from frames transmitted on the wireless network;

(b) receiving scan data comprising information collected from frames transmitted on the wireless network, wherein the scan data is associated with monitoring of one or more wireless access points, one or more wireless network nodes or combinations thereof;

(c) identifying a relationship (i) between at least one of the wireless access points and at least one of the wireless network nodes or (ii) between any two wireless network nodes based on the received scan data, a characteristic of at least one of the wireless access points, a characteristic of at least one of the wireless network nodes or combinations thereof, wherein the relationship is identified responsive to an analysis of the scan data and responsive to a relationship between the wireless sensor and a server;

(d) storing the identified relationship, access point characteristic, node characteristic or combinations thereof as topology data; and

(e) formatting topology data generated based upon a desired output format;

(f) outputting the formatted topology data to a desired output device; and

(g) comparing the topology data to prior topology data to evaluate potential security and policy violations of the wireless network, wherein the comparing comprises one of a rules-based comparison, a pattern matching-based comparison, and a combination thereof.